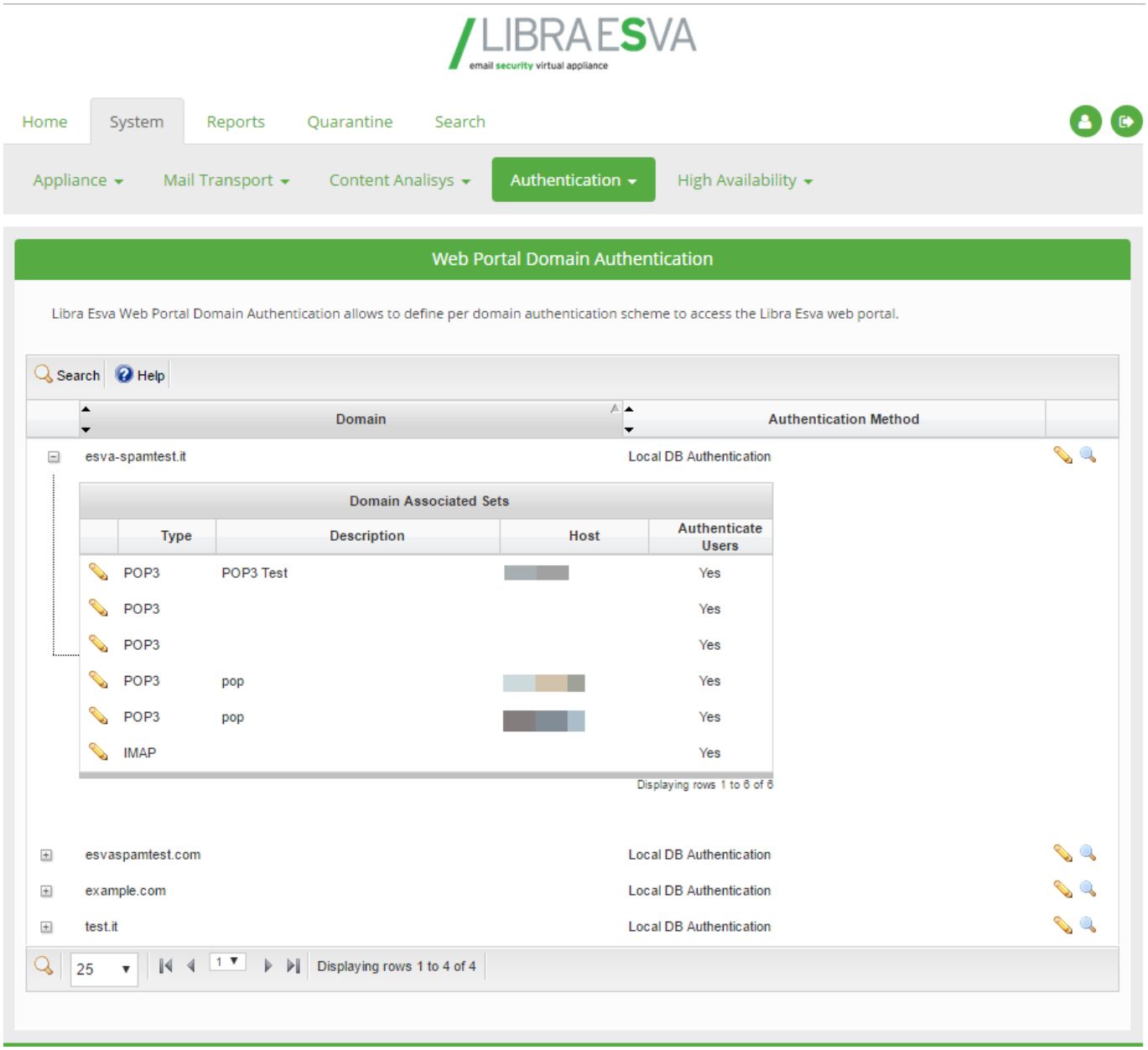
Web Portal Domain Authentication

This section allows to configure how the web portal can be accessed.

Domain Authentication

Libraesva ESG relies on a per domain authentication mechanism.

From this tab you can define how each hosted domain is authenticated when logging in on the Libraesva ESG Web Portal.



You can choose from one of the followings:

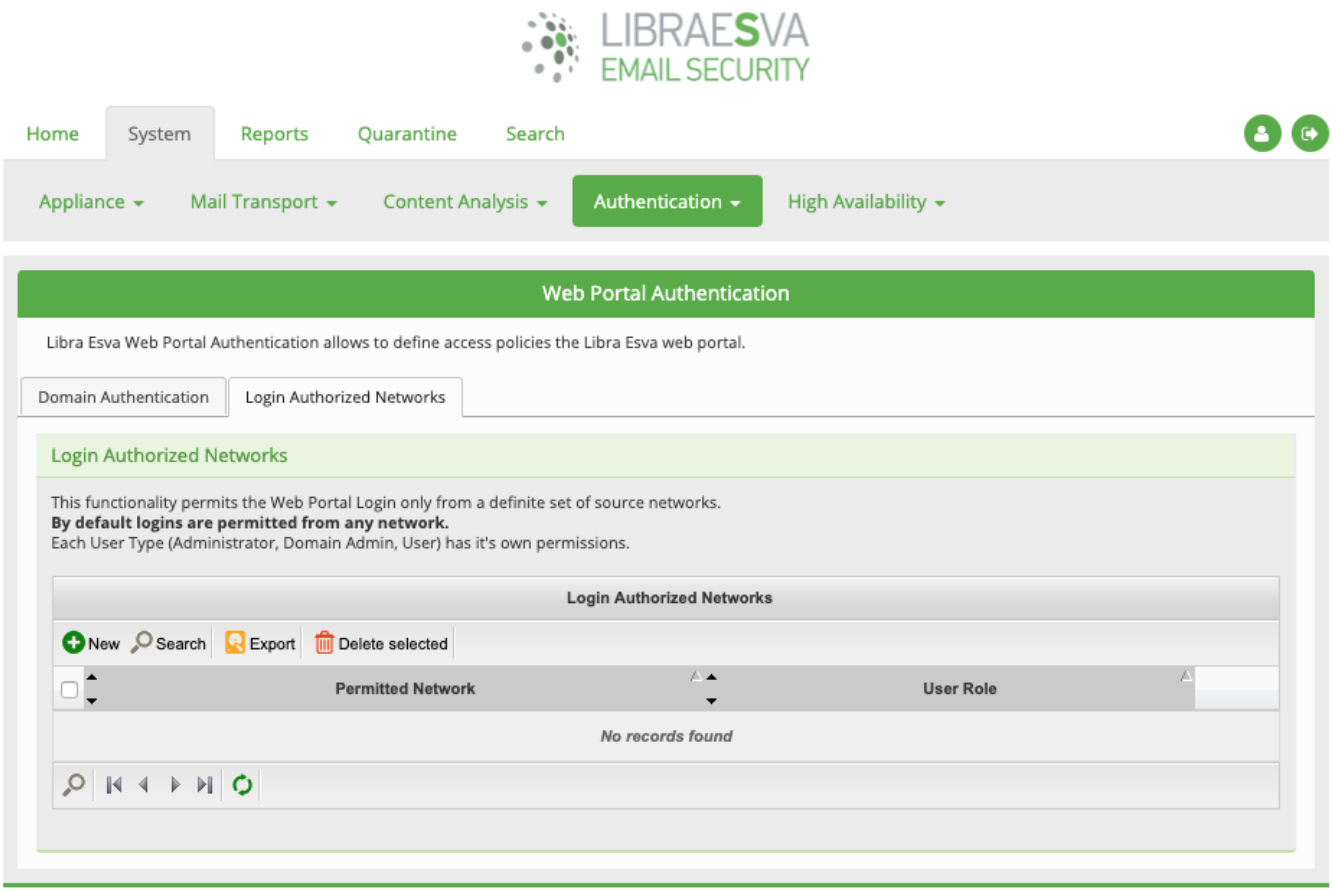
- **“No Access”** means that the users belonging to this domain will be locked out from the web interface.
- **“Local DB Authentication”** means that user’s password is stored locally on ESG DB. Users are created locally from *System->User Management*
- **“Ldap Authentication”** means that user’s password is stored on a LDAP server. The login username has to be the user main email address as mapped in the LDAP set. The email domain is used to correctly identify the user associated LDAP server in LDAP dataset List. At least one LDAP set must be defined and active.
- **“Pop3 Authentication”** means that user’s password is stored on the POP3 server. Obviously, also in this case, the login username has to be the user email address. At least one POP3 set must be defined and active.
- **“IMAP Authentication”** means that user’s password is stored on the IMAP server. Obviously, also in this case, the login username has to be the user email address. At least one IMAP set must be defined and active.
- **“Office 365 Authentication”** means that user’s password is stored on the Office365 Tenant. Obviously, also in this case, the login username has to be the user email address. At least one Office365 must be defined and active.
- **“Google Authentication”** means that user’s password is stored on the Gsuite Tenant. Obviously, also in this case, the login username has to be the user email address. At least one Google Configuration must be defined and active.

When choosing any authentication method other than Local, it’s handy to see which sets are already associated to each domain. By clicking the + icon on the left you can expand and check LDAP, POP3, IMAP sets defined for the domain.

×**NOTE:** default authentication scheme is always Local.

Login Authorized Networks

This section permits to restrict the portal access login, making it working only if the request originates from a definite set of networks or IPs.



To restrict web portal access:

1. Click **New**
2. Enter the permitted source network
3. Specify the user role: Administrator, Domain Admin, User
4. Click **Save**

For example to restrict admin access only if the portal is accessed from the IP 1.2.3.4 enter:

Permitted Network: 1.2.3.4/32

User Role: Administrators

×**NOTE: b**y default logins are permitted from any network, for all user types.